ICS-CERT ALERT

ICS-ALERT-12-097-02A—3S-SOFTWARE CODESYS IMPROPER ACCESS CONTROL

UPDATE A

October 26, 2012

ALERT

SUMMARY

ICS-CERT is aware of a public report of improper access control vulnerability affecting 3S-Software CoDeSys. CoDeSys is a third-party product used on programmable logic controllers (PLCs) and engineering workstations. According to this report, an attacker can upload unauthenticated configuration changes to the PLC, which may include arbitrary code. This report was released by Reid Wightman, [Digital Bond] (now with IOActive), without coordination with either the vendor or ICS-CERT.

ICS-CERT has notified the affected vendor of the report and has asked the vendor to confirm the vulnerabilities and identify mitigations. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks.

--------- Begin Update A Part 1 of 2 --------

The researchers have publicly released two tools containing exploit code for these vulnerabilities. The first tool can be used by an attacker to obtain a shell on the PLC. The second tool can be used by an attacker to transfer arbitrary files to and from the PLC.

The report included vulnerability details for the following vulnerabilities:

Vulnerability Type	Remotely Exploitability	Impact
Improper Access Control	Yes	Loss of integrity, confidentiality, availability
Directory Traversal	Yes	Loss of integrity, confidentiality

Please report any issues affecting control systems in critical infrastructure environments to ICS-CERT.

--------- End Update A Part 1 of 2----------

MITIGATION

--------- Begin Update A Part 2 of 2 --------

3S has a Web site where asset owners can look up devices that uses CoDeSys. http://www.3s-software.com/index.shtml?codesys_dev_dir.

--------- End Update A Part 2 of 2----------

ICS-CERT is currently coordinating with the vendor and security researcher to identify mitigations.

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[a]
- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- If remote access is required, employ secure methods such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

ICS-CERT also provides a recommended practices section for control systems on the US-CERT Web site. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[b]

Organizations that observe any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

ICS-CERT CONTACT

ICS-CERT Operations Center
1-877-776-7585
ics-cert@hq.dhs.gov

For industrial control systems security information and incident reporting: www.ics-cert.org

a. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, Web site last accessed October 25, 2012.

b. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Website last accessed October 25, 2012.

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

DOCUMENT FAQ

What is an ICS-CERT Alert? An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.